DEPARTMENT OF DEFENSE

DoD Enterprise Architecture Technical Reference Model

v0.04

20 August 2005

By

DoD EA Congruence Community of Practice

TABLE OF CONTENTS

DoD EA Technical Reference Model

INTRODUCTION

To facilitate efforts to transform the Department of Defense (DoD)—and in conjunction with the Federal Government's efforts to transform government to be citizen-centered, results-oriented, and market-based—the DoD is aligning its Enterprise Architecture Reference Models with the OMB Federal Enterprise Architecture Reference Models ((FEA RMs). The FEA RMs are a business-based framework for Government-wide improvement. The FEA is being constructed through a collection of interrelated reference models designed to facilitate cross-agency analysis and the identification of duplicate investments, gaps, and opportunities for collaboration within and across Federal agencies. DoD is developing a similar set of reference models to facilitate net-centric transformation, re-use, as well as EA alignment to the FEA RMs. The discussion of the DoD Enterprise Architecture Technical Reference Model (DoD EA TRM) follows.

The DoD EA TRM outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (service components) that may be used and leveraged to support DoD electronic Government (e-Gov) initiatives in a component-based or service-oriented architecture. The DoD EA TRM unifies existing technical standard references developed by DoD Components and e-Gov guidance. Thus, it provides a foundation to advance the re-use of technology and component services from a DoD-wide and, ultimately, a Government-wide perspective.

STRUCTURE OF THE DOCUMENT

The document is organized according to the following chapters:

***Chapter* 1** defines and describes the DoD EA TRM.

***Chapter* 2** describes the structure of the DoD EA TRM.

***Chapter* 3** is a mapping between DoD Information Technology Standards Registry (DISR) and the FEA TRM.

Chapter 4 discusses the use and maintenance of the DoD EA TRM.

Chapter 5 is an analysis of the DoD EA TRM with conclusion and recommendations.

***Appendix* A** contains two tables that map the DoD specifications to FEA TRM standards and specifications and vice versa.

Chapter 1. DoD EA TRM Overview

PURPOSE AND PHILOSOPHY

Adopting the FEA TRM philosophy, the DoD EA TRM outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (service components) that may be used and leveraged in a component-based or service-oriented architecture (SOA) and to support DoD's e-Gov initiatives. With this SOA focus, the DoD EA TRM is intended primarily to facilitate the DoD transition to net-centricity. It may also provide value, however, in helping to identify areas of technology overlap and potential simplification in legacy and stovepipe applications.

The DoD EA TRM serves to outline the technology elements that collectively support the adoption and implementation of component-based architectures in DoD. The model provides the foundation to advance the re-use of technology and component services across DoD and the Federal Government through standardization. Aligning DoD capital investments to the DoD EA TRM leverages a common, standardized vocabulary, allowing inter-DoD, inter-agency, intra-DoD, and intra-agency discovery, collaboration, and interoperability. DoD and other cabinet agencies, and the Federal Government, might benefit from economies of scale by identifying and re-using the best solutions and technologies to support their business functions, missions, and target architectures.

The DoD EA TRM is not intended to replace any of the DoD standards sources, such as the DOD IT Standards Registry (DISR). Instead, the TRM pulls from, and integrates, these sources in a specific format designed to assist DoD program and investment decisions, and facilitates mapping to the FEA TRM. More specifically, the DoD EA TRM was formed to:

- Create a DoD-wide EA TRM that aligns with the FEA TRM.
- Create a DoD-wide reference model that unifies DoD Component TRMs and the FEA TRM.
- Focus on technology standards and specifications that embrace the Internet and related approaches such as a net-centric environment
- Create a foundation that focuses heavily on the secure delivery and construction of service components and their interfaces
- Identify the layers of a component-based architecture (CBA) and relevant supporting technologies

KEY CONCEPTS AND DEFINITIONS

Technologies – refers to a specific implementation of a standard within the context of a given specification.

The following illustrates the use of the term 'technologies' in the DoD EA TRM:

- PL/SQL is an Oracle implementation of the SQL Standard.
- ISQL/w is a Microsoft implementation of the SQL Standard.
- ODBC is an implementation of a data access standard within various relational database vendor specifications.

- JDBC is an implementation of a data access standard within the Sun Java specification.

While all are based on an Open Standard, each vendor has its own implementation of the standard based on its own technologies.

Legacy - refers to software and/or hardware from previous technology generations.

Component - a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface.

Component-based Architecture **(CBA)** – a technology architecture comprised of run-time services and control structures together with an application infrastructure. The CBA consists of the component model and the architecture services that are built around the model. Solutions based on a CBA are more dynamic, flexible, and easier to maintain than traditional monolithic solutions.

Capability – the ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms. A capability includes the doctrine, organization, training, materiel, leadership and education, personnel, and facilities required to achieve a specified course of action.

Specification - a document prepared to support acquisition that describes the essential technical requirements for purchased materiel and the criteria for determining whether those requirements are met. A specification is a version or instantiation of a specific standard (e.g. area of standardization). (DoD 4120.3-M)

Figure 1 shows the evolution from monolithic to component-based solutions, as they have progressed over the years, thus bringing us to the new millennium with the characteristics seen in the figure.

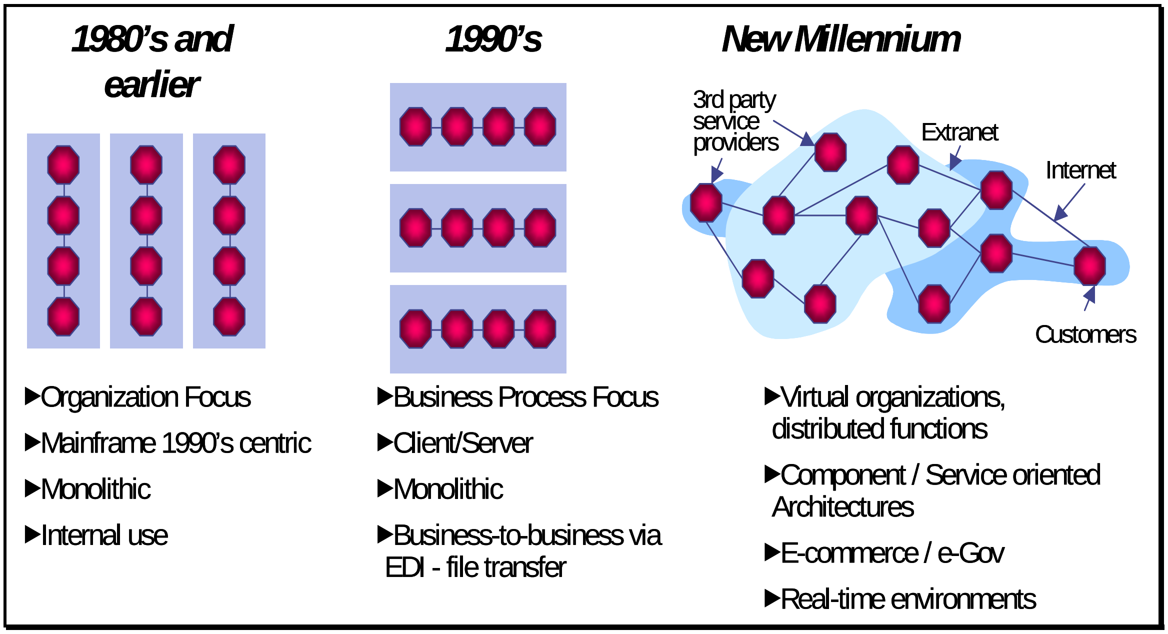


Figure 1: Evolution of Monolithic and Component-Based Solutions

USING THE FEA TRM ORGANIZATIONAL SCHEME

In this document, the DoD EA TRM uses the FEA TRM organizational scheme as the foundation for its mapping. We first mapped the DoD standards and specifications in the DISR previously known as the Joint Technical Architecture (JTA) to the standards in the FEA TRM. The initial mapping revealed standards that were in the FEA TRM but not in DISR, and vice versa, thus leading to a gap analysis between the two sets of standards. Technical standards and specifications applicable to DoD but not present in the FEA TRM are highlighted in *red italic* below.

While the current DoD Technical Reference Model DoD TRM) provided the organizational scheme for the DoD standards in the JTA, the DoD TRM in its current state does not reflect the transformation goals of the Department toward net-centricity and must be changed. Organizing the DoD EA TRM around the FEA TRM, and perhaps augmenting the DoD EA TRM with other specific standards for accommodating DoD Domain specific and DoD telecommunications requirements (if necessary in a net-centric environment), may lead to the evolution of a new net-centric DoD EA TRM. In the meantime the following analysis will lead to conclusions and recommendations to address this and other standard alignment issues between the DoD EA TRM and the FEA TRM and will inform management decision makers at both the DoD and Federal levels as DoD and the Federal Government move toward a more net-centric environment. A net-centric environment will enhance the entire government's capabilities to combat global terrorism and other threats to national security and other national interests world-wide.

DEVELOPMENT OF THE DOD EA TRM

In developing the DoD EA TRM, the FEA Congruence Working Group built on the foundation of the work by the FEA PMO, which leveraged previous Federal architecture efforts to guide the design of the government-wide model. The DoD capitalized on extensive research by the FEA PMO on industry and government standards, specifications, and technologies to further refine and enhance the DoD EA TRM.

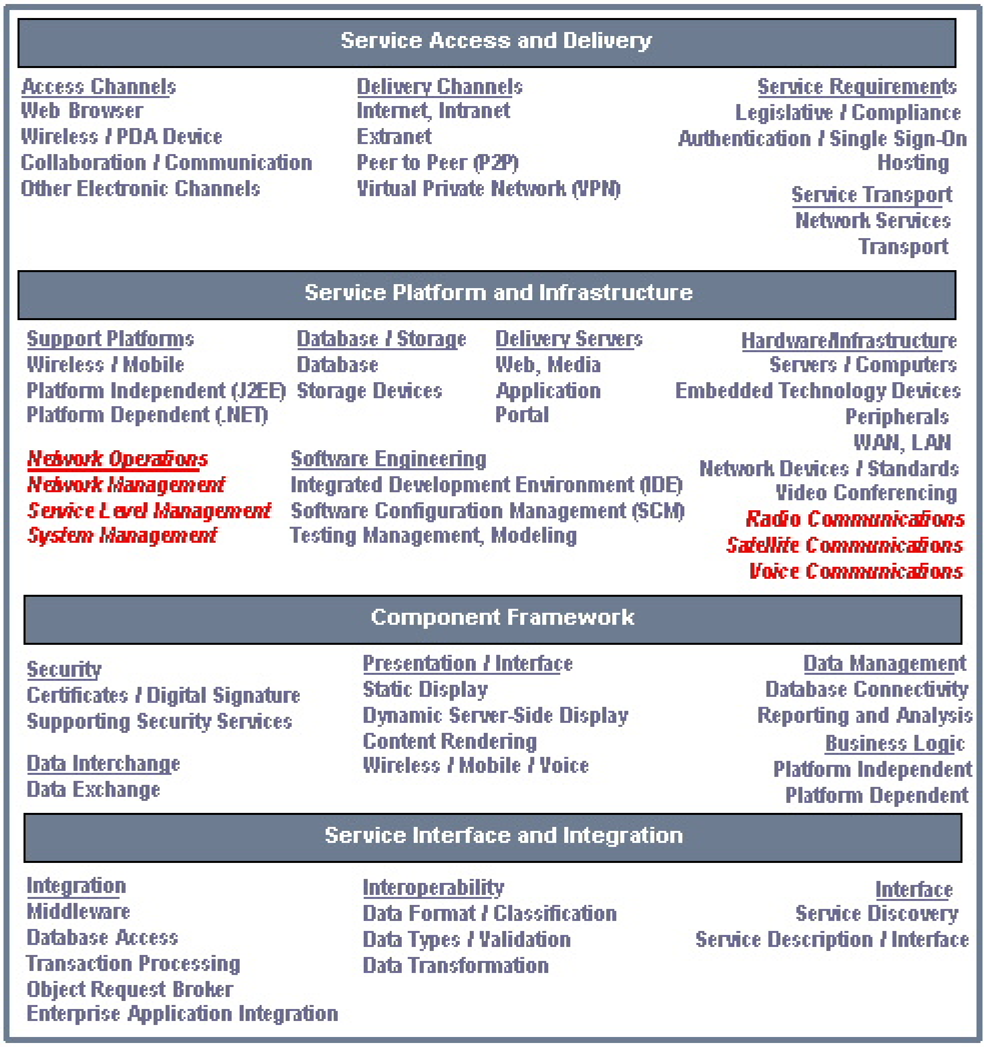
The information contained within these sources provided thorough documentation of the many services, capabilities, and technologies that industry and government applications and IT initiatives deliver. Building on the FEA PMO normalization and categorization of standards, specifications, and technologies that support the business and service components and capabilities, the DoD proceeded to develop its own DoD EA TRM.

Once a list of Service Areas, Service Representations, Service Categories, and Specifications was developed, definitions were given to each of the layers of the model and their contents. These were used as the organizational scheme to compare and contrast DoD's EA TRM specifications, definitions and contents to the FEA TRM equivalents. Continued refinements of the DoD EA TRM will include factoring in DoD future architecture visions such as the Global Information Grid (GIG) architecture; Business Enterprise Architecture (BEA); warfighter architectures; the Net-Centric Operations and Warfare Reference Model (NCOW RM); as well as information from the DoD Architecture Framework (DoDAF) product renderings and the Core Architecture Data Model (CADM).

VENDOR-SPECIFIC PRODUCTS

The DoD EA TRM is not intended to provide or endorse particular vendor products. Some specific products are listed in detailed mapping tables included with the TRM. These are products sanctioned by the Federal CIO Council, and specifically pertain to developing Web solutions, as do all of the technologies, standards, and specifications contained within the FEA TRM. For example, if you see a product such as Microsoft .NET within the DoD EA TRM mapping tables, it is because that product is on the CIO Council list of products that are used for developing Web pages and Web service/component-based solutions, a component of CBA.

CHAPTER 2. STRUCTURE OF THE DOD EA TRM



Service Access and Delivery

Access Channels
Web Browser
Wireless / PDA Device
Collaboration / Communication
Other Electronic Channels

Delivery Channels
Internet, Intranet
Extranet
Peer to Peer (P2P)
Virtual Private Network (VPN)

Service Requirements
Legislative / Compliance
Authentication / Single Sign-On
Hosting

Service Transport
Network Services
Transport

Service Platform and Infrastructure

Support Platforms
Wireless / Mobile
Platform Independent (J2EE)
Platform Dependent (.NET)

Database / Storage
Database
Storage Devices

Delivery Servers
Web, Media
Application
Portal

Hardware/Infrastructure
Servers / Computers
Embedded Technology Devices
Peripherals
WAN, LAN
Network Devices / Standards
Video Conferencing
Radio Communications
Satellite Communications
Voice Communications

Network Operations
Network Management
Service Level Management
System Management

Software Engineering
Integrated Development Environment (IDE)
Software Configuration Management (SCM)
Testing Management, Modeling

Component Framework

Security
Certificates / Digital Signature
Supporting Security Services

Data Interchange
Data Exchange

Presentation / Interface
Static Display
Dynamic Server-Side Display
Content Rendering
Wireless / Mobile / Voice

Data Management
Database Connectivity
Reporting and Analysis

Business Logic
Platform Independent
Platform Dependent

Service Interface and Integration

Integration
Middleware
Database Access
Transaction Processing
Object Request Broker
Enterprise Application Integration

Interoperability
Data Format / Classification
Data Types / Validation
Data Transformation

Interface
Service Discovery
Service Description / Interface

Figure 2: DoD EA Technical Reference Model (TRM)

The DoD EA TRM is organized into four (4) core Service Areas, each with supporting service categories, and each service category with supporting standards, as shown in **Figure 2**. This parallels the FEA TRM organization structure. The DoD EA TRM aligns very closely to the FEA TRM. Several additional categories have been added to the DoD EA TRM, all of which are highlighted in *red italic* in the diagrams and text body of this document. Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas. The four (4) Service Areas within the DoD EA TRM are:

- **Service Access and Delivery**— refers to the collection of standards and specifications to support external access, exchange, and delivery of service components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific service component.

- ***Service Platform & Infrastructure***—refers to the collection of delivery and support platforms, infrastructure capabilities, and hardware requirements to support the construction, maintenance, and availability of a service component or capabilities.
- ***Component Framework***—refers to the underlying foundation, technologies, standards, and specifications by which service components are built, exchanged, and deployed across service–oriented architectures.
- ***Service Interface and Integration***—refers to the collection of technologies, methodologies, standards, and specifications that govern how agencies will interface (internally and externally) with a service component. This area also defines the methods by which components will interface and integrate with back office / legacy assets.

Each Service Area, as illustrated in **Figure 2**, consists of multiple Service Categories, Service Standards, and Service Specifications that provide the foundation to group standards, specifications, and technologies that directly support the Service Area.

Supporting each Service Area is a collection of Service Categories. Service Categories are used to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve. Each Service Category is supported by one or more Service Standards.

Service Standards are used to define the standards and technologies that support the Service Category. The final level of the DoD EA TRM is the Service Specification layer that details the specification and / or provider of the Service Standard specification. **Figure 3** shows the relationship of Service Areas, Service Categories, standards, and specifications.

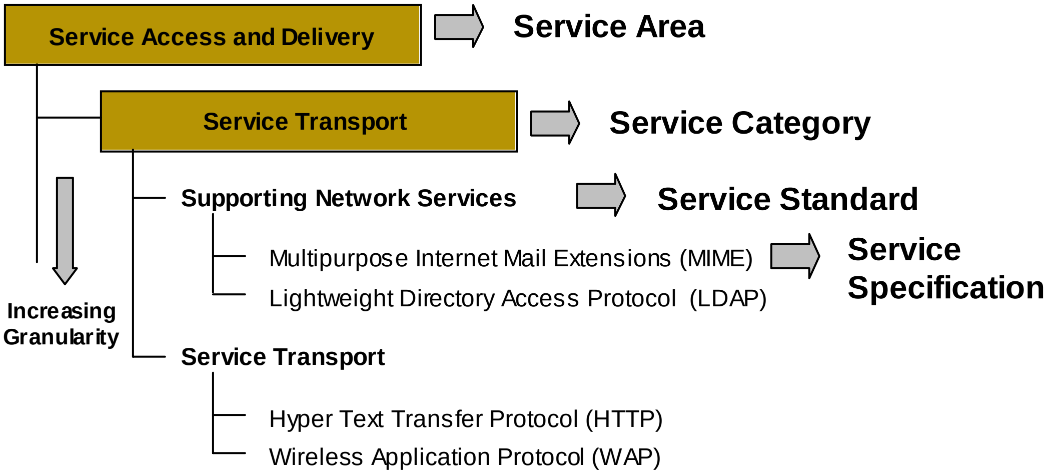

Service Access and Delivery
Service Area
Service Transport
Service Category
Supporting Network Services
Service Standard
Multipurpose Internet Mail Extensions (MIME)
Lightweight Directory Access Protocol (LDAP)
Service Specification
Increasing Granularity
Service Transport
Hyper Text Transfer Protocol (HTTP)
Wireless Application Protocol (WAP)

Figure 3: Service Area, Category, Standard, and Specification Hierarchy

As depicted in **Figure 4**, each Service Area, and supporting Service Categories, can be structured across typical network topologies that provide clear distinctions between External Environments, Demilitarized Zones (DMZ), or Internal Environments housing back-office and legacy assets.

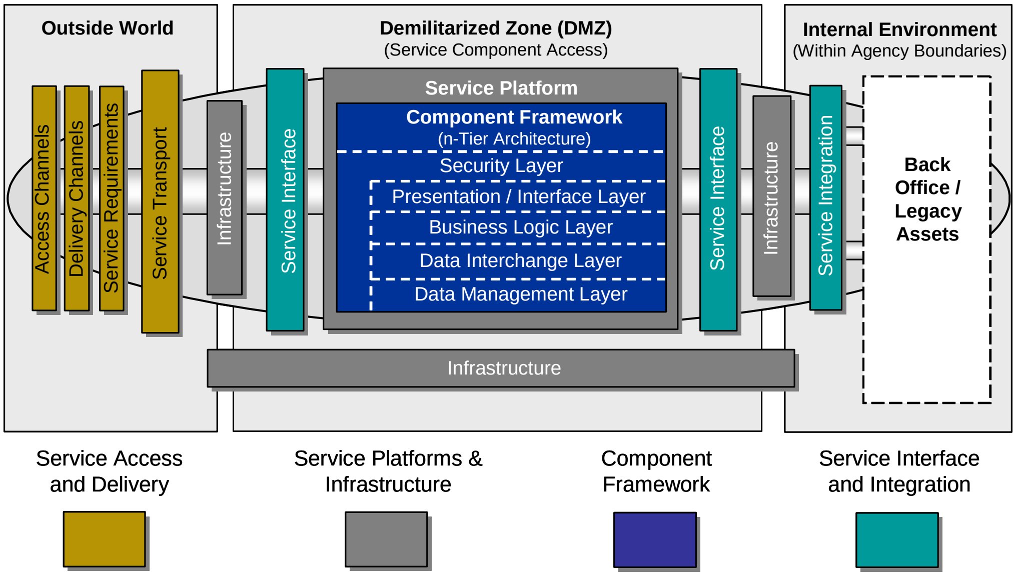


Figure 4: TRM Within A Typical Network Topology

SERVICE ACCESS AND DELIVERY

The Service Access and Delivery Service Area, as illustrated in **Figure 5**, defines the collection of Access and Delivery Channels that will be used to utilize the service component, and the legislative requirements that govern its use and interaction.

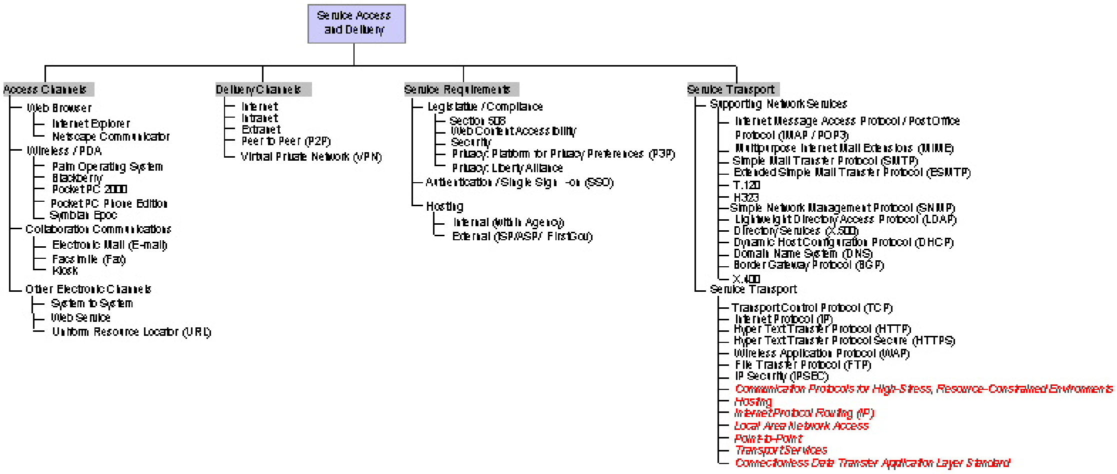

Service Access and Delivery
Access Channels
Web Browser
Internet Explorer
Netscape Communicator
Wireless / PDA
Palm Operating System
Blackberry
Pocket PC 2000
Pocket PC Phone Edition
Symbian Epoc
Collaboration Communications
Electronic Mail (E-mail)
Facsimile (Fax)
Kiosk
Other Electronic Channels
System to System
Web Service
Uniform Resource Locator (URL)
Delivery Channels
Internet
Intranet
Extranet
Peer to Peer (P2P)
Virtual Private Network (VPN)
Service Requirements
Legislative / Compliance
Section 508
Web Content Accessibility
Security
Privacy: Platform for Privacy Preferences (P3P)
Privacy: Liberty Alliance
Authentication / Single Sign -on (SSO)
Hosting
Internal (within Agency)
External (ISP/ASP/ FirstGov)
Service Transport
Supporting Network Services
Internet Message Access Protocol / Post Office Protocol (IMAP / POP3)
Multipurpose Internet Mail Extensions (MIME)
Simple Mail Transfer Protocol (SMTP)
Extended Simple Mail Transfer Protocol (ESMTP)
T.120
H323
Simple Network Management Protocol (SNMP)
Lightweight Directory Access Protocol (LDAP)
Directory Services (X.500)
Dynamic Host Configuration Protocol (DHCP)
Domain Name System (DNS)
Border Gateway Protocol (BGP)
X.400
Service Transport
Transport Control Protocol (TCP)
Internet Protocol (IP)
Hyper Text Transfer Protocol (HTTP)
Hyper Text Transfer Protocol Secure (HTTPS)
Wireless Application Protocol (WAP)
File Transfer Protocol (FTP)
IP Security (IPSEC)
Communication Protocols for High-Stress, Resource-Constrained Environments
Hosting
Internet Protocol Routing (IP)
Local Area Network Access
Point-to-Point
Transport Services
Connectionless Data Transfer Application Layer Standard

Figure 5: Service Access and Delivery Service Area

The Service Access and Delivery Service Categories, Standards, and Specifications are defined below:

Access Channels

Access Channels define the interface between an application and its users, whether it is a browser, personal digital assistant, or other medium.

Web Browser – Define the program that serves as your front end to the World Wide Web (WWW)on the Internet. In order to view a site, type its address (URL) into the browser's location field.

Wireless / PDA - Define the technologies that use transmission via the airwaves. Personal Digital Assistant (PDA) is a handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, to-do list, and note taker.

Collaboration Communications – Define the forms of electronic exchange of messages, documents, or other information. Electronic communication provides efficiency through expedited time-of-delivery.

Electronic Mail (E-mail) – E-mail (electronic mail) is the exchange of computer-generated and stored messages by telecommunication. An e-mail can be created manually via messaging applications or dynamically, programmatically such as by automated response systems.

Facsimile (Fax) – A fax is the digitized image of text and/or pictures, represented as a series of dots (bit map). Faxes are sent and received through telecommunication channels such as telephone or Internet.

Kiosk - A kiosk is a small physical structure (often including a computer and a display screen) that displays information. Kiosks are common in public buildings. Kiosks are also used at trade shows and professional conferences.

Other Electronic Channels – Define the other various mediums of information exchange and interface between a user and an application.

System to System - System to System involves at least two computers that exchange data or interact with each other independent of human intervention or participation.

Web Service - Web services (sometimes called application services) are services (usually including some combination of programming and data, but possibly including human resources as well) that are made available from a business's Web server for Web users or other Web-connected programs.

Uniform Resource Locator (URL) – URL is the global address of documents and other resources on the WWW. The first part of the address indicates what protocol to use (i.e., “http://”), and the second part specifies the IP address or the domain name where the resource is located (i.e., “www.firstgov.gov”).

Delivery Channels

Delivery Channels define the level of access to applications and systems based upon the type of network used to deliver them.

Internet - The Internet is a worldwide system of computer networks in which users at any one computer can, if they have permission, get information from any other computer.

Intranet - An intranet is a private network that is contained within an enterprise. It may consist of many inter-linked local area networks and is used to share company information and resources among employees.

Extranet - An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

Peer to Peer (P2P) - Peer to peer represents a class of applications—operating outside the DNS system and have significant or total autonomy from central servers—that take advantage of resources available on the Internet.

Virtual Private Network (VPN) - A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Service Requirements

Service Requirements define the necessary aspects of an application, system or service to include legislative, performance, and hosting.

Legislative / Compliance - Defines the pre-requisites that an application, system, or service must have mandated by Congress or governing bodies.

Section 508 – Section 508 requires that Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public.

Web Content Accessibility - Refers to hardware and software that helps people who are physically or visually impaired.

Security - Policy and procedures that protect data against unauthorized access, use, disclosure, disruption, modification, or destruction.

Privacy: Platform for Privacy Preferences (P3P) – A specification that will allow users' Web browsers to automatically understand Web sites' privacy practices. Privacy policies will be embedded in the code of a Web site. Browsers will read the policy then automatically provide certain information to specific sites based on the preferences set by the users. For instance, if the site is an e-commerce site, the browser will automatically provide shipping info. If the site is requesting demographic info, then the browser will know to provide it anonymously. The P3P specification was developed by the W3C P3P Syntax, Harmonization, and Protocol Working Groups, including W3C member organizations and experts in the field of Web privacy. P3P is based on W3C specifications that have already been established, including HTTP, XML and Resource Description Framework (RDF). *Privacy* is policy that deals with the degree to which an individual can determine which personal information is to be shared with whom and for what purpose. http://www.w3.org/P3P/

Privacy: Liberty Alliance – The Liberty Alliance Project is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. A federated network identity model will enable every business or user to manage their own data, and ensure that the use of critical personal information is managed and distributed by the appropriate parties, rather than a central authority. *Privacy* is policy that deals with the degree to which an individual can determine which personal information is to be shared with whom and for what purpose. http://www.projectliberty.org/

Authentication / Single Sign-on (SSO) – Refers to a method that provides users with the ability to log-in one time and get authenticated access to all their applications and resources.

Hosting – Refers to the service provider who manages and provides availability to a web site or application, often bound to a Service Level Agreement (SLA). The Hosting entity generally maintains a server farm with network support, power backup, fault tolerance, load-balancing, and storage backup.

Internal (within Agency) – The hosting of a web site or application within an Agency. The Agency is responsible for the maintenance, support and availability of the web site or application.

External (ISP/ASP/FirstGov) – The outsourcing of a web site or application with a managed service provider. An Internet Service Provider (ISP) provides telecommunications circuits, server co-location, and web site and application hosting. An Application Service Provider (ASP) offers software-based services for high-end business applications and specific-needs applications such as payroll, sales force automation, and human resources. FirstGov is the official managed service provider for the Federal Government.

Service Transport

Service Transport defines the end-to-end management of the communications session to include the access and delivery protocols.

Supporting Network Services - These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.

Internet Message Access Protocol / Post Office Protocol (IMAP / POP3) – IMAP allows a client to access and manipulate electronic mail messages on a server. IMAP permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP also provides the capability for an offline client to resynchronize with the server. POP3 is the most commonly used protocol for retrieving e-mail from a mail host.

Multipurpose Internet Mail Extensions (MIME) – MIME extends the format of Internet mail to allow non-US- American Standard Code for Information Interchange (ASCII) textual messages, non-textual messages, multi-part message bodies, and non-US-ASCII information in message headers. MIME support allows compliant email clients and servers to accurately communicate embedded information to internal and external users.

Simple Mail Transfer Protocol (SMTP) – SMTP facilitates transfer of electronic-mail messages. It specifies how two systems are to interact, and the format used to control the transfer of electronic mail.
Extended Simple Mail Transfer Protocol (ESMTP) - ESMTP allows new service extensions to SMTP to be defined and registered with Internet Assigned Numbers Authority (IANA).

T.120 – T.120, an International Telecommunications Union (ITU) standard, contains a series of communication and application protocols and services that provide support for real-time, multipoint data communications. These multipoint facilities are important building blocks for collaborative applications, including desktop data conferencing and multi-user applications.

H.323 – H.323, an International Telecommunications Union (ITU) standard, addresses Video (Audiovisual) communication on Local Area Networks, including Corporate Intranets and packet-switched networks generally.

Simple Network Management Protocol (SNMP) - SNMP eliminates several of the security vulnerabilities in earlier version.

Lightweight Directory Access Protocol (LDAP) - LDAP is a subset of X.500 designed to run directly over the TCP/IP stack. LDAP is, like X.500, an information model and a protocol for querying and manipulating it. LDAPv3 is an update developed in the IETF (Internet Engineering Task Force), which address the limitations found during deployment of the previous version of LDAP.

Directory Services (X.500) – This is a network service that discovers and identifies resources on a network and makes them accessible to users and applications. The resources include users, e-mail addresses, computers, mapped drives, shared folders, and peripherals such as printers and PDA docking stations. Users and computers access these resources without needing to know how or where the resources are connected.

Dynamic Host Configuration Protocol (DHCP) – A protocol for assigning dynamic IP addresses to devices on a network. A device can receive a different IP address for every connection. Dynamic addressing provides reduced network administration over deploying and connecting user and peripheral devices.

Domain Name System (DNS) – A protocol used for translating domain names (i.e. www.feapmo.gov) to their respective IP addresses. DNS is collectively a network of devices which store query results. As one DNS server or device cannot provide the translated IP address, it queries other DNS devices. This process is invisible to the user.

Border Gateway Protocol (BGP) – Refers to a routing protocol used to exchange routing information between routers on a network, enabling more efficient routing of data.

X.400 – An ISO and ITU standard for e-mail message addressing and transporting. X.400 supports Ethernet, X.25, TCP/IP and dial-up transport methods.

Service Transport - These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.

Transport Control Protocol (TCP) - TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the destination.

Internet Protocol (IP) - This is the protocol of the Internet and has become the global standard for communications. IP accepts packets from TCP, adds its own header and delivers a "datagram" to the data link layer protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

Hyper Text Transfer Protocol (HTTP) - The communications protocol used to connect to servers on the World Wide Web. It's primary function is to establish a connection with a web server and transmit HTML pages to the client browser.

Hyper Text Transfer Protocol Secure (HTTPS) - The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol.

Connectionless Data Transfer Application Layer Standard - The Connectionless Data Transfer Application Layer Standard allows Variable Message Format (VMF) messages to be used in connectionless applications. This standard uses User Datagram Protocol (UDP) as a transport service.

Wireless Application Protocol (WAP) - The Wireless Application Protocol (WAP) is an open, global specification that empowers users of digital mobile phones, pagers, personal digital assistants and other wireless devices to securely access and interact with Internet/intranet/extranet content, applications, and services.

File Transfer Protocol (FTP) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server using FTP.

IP Security (IPSEC) – A set of protocols used to secure IP packet exchange. Tunnel and Transport are the two (2) modes supported by IPSEC. IPSEC uses certificates and Public Keys to authenticate and validate the sender and receiver.

Communication Protocols for High-Stress, Resource-Constrained Environments - DoD entered a cooperative effort in September 1997 with the National Aeronautics and Space Administration (NASA) and the National Security Agency (NSA) to develop Internet-based protocols for "stressed" communications links. Such links are characterized by one or more of high bit error rates, long delays, low bandwidths, and high degrees of asymmetry. This work is also applicable for systems with limited computer processing power.

Hosting - Hosts are computers that generally execute application programs on behalf of users and share information with other hosts. Internet Engineering Task Force (IETF) Standard 3 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. IETF Standard 3 also adds additional discussion and guidance for implementers. IETF Standard 3 consists of Request for Comments (RFC) 1122 and RFC 1123. This pair of documents defines and discusses the requirements for host system implementations of the IP suite. RFC 1122 covers the communications protocol layers (i.e., link layer, IP layer, and transport layer). RFC 1123 covers the application layer protocols.*Internet Protocol Routing (IP)* - Routers exchange connectivity information with other routers to determine network connectivity and adapt to changes in the network. This enables routers to determine, on a dynamic basis, where to send IP packets.

Local Area Network Access - While no specific LAN technology is mandated, the following is required for interoperability in a joint environment. This requires provision for a LAN interconnection. Ethernet, the implementation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD), is the most common LAN technology in use with TCP/IP. The hosts use a CSMA/CD scheme to control access to the transmission medium. An extension to Ethernet, Fast Ethernet provides interoperable service at both 10 Mbps and 100 Mbps. Higher-speed interconnections are provided by 100BASE-TX (two pairs of Category 5 unshielded twisted pair, with 100BASE-TX Auto-Negotiation features employed to permit interoperation with 10BASE-T).

Point-to-Point - The point-to-point standards are designed for single links that transport packets between two peers. These links provide full-duplex, simultaneous, bi-directional operation, and are assumed to deliver packets in order.

Transport Services - The transport services provide host-to-host communications capabilities for application support services. The following sections define the requirements for this service.

SERVICE PLATFORM AND INFRASTRUCTURE

The Service Platform and Infrastructure Area, as illustrated in **Figure 6**, defines the collection of platforms, hardware and infrastructure specifications that enable Component-Based Architectures and Service Component re-use.

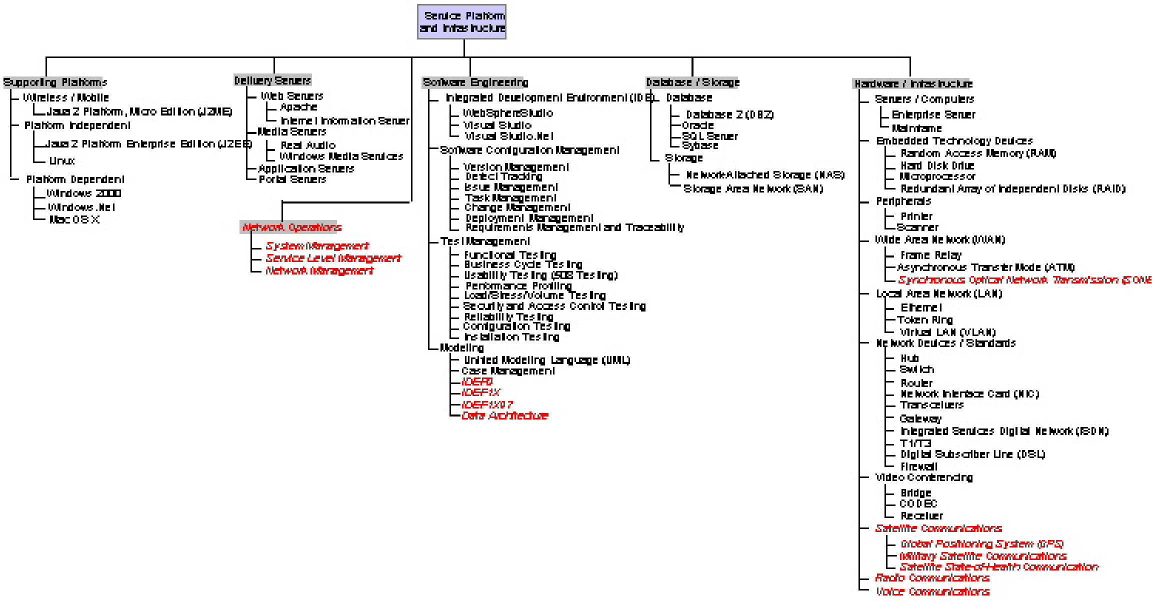


Figure 6: Service Platform and Infrastructure Service Area

The Service Platform and Infrastructure Service Categories, Standards, and Specifications are defined below:

Supporting Platforms

Supporting platforms are hardware or software architectures. The term originally dealt with only hardware, and it is still used to refer to a CPU model or computer family.

Wireless / Mobile - Radio transmission via the airwaves. Various communications techniques are used to provide wireless transmission including infrared line of sight, cellular, microwave, satellite, packet radio and spread spectrum.

Platform Independent - Defines the operating systems and programming languages that are able to execute and run on any platform or operating system. A platform is the underlying hardware and software comprising a system.

Platform Dependent - Defines the operating systems and programming languages that are able to execute and run on a specific platform or operating system. A platform is the underlying hardware and software comprising a system.

Delivery Servers

Delivery Servers are front-end platforms that provide information to a requesting application. It includes the hardware, operating system, server software, and networking protocols.

Web Servers – A computer that provides World Wide Web services on the Internet. It includes the hardware, operating system, Web server software, TCP/IP protocols and the Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server."

Media Servers – Provide optimized management of media-based files such as audio and video streams and digital images.

Application Servers – In a three-tier environment, a separate computer (application server) performs the business logic, although some part may still be handled by the user's machine. After the popularity of the Web exploded in the mid 1990s, application servers became Web–based.

Portal Servers – Portals represent focus points for interaction, providing integration and single-source corporate information.

Software Engineering

Software engineering covers not only the technical aspects of building software systems, but also management issues, such as testing, modeling and versioning.

Integrated Development Environment (IDE) – This consists of the hardware, software and supporting services that facilitate the development of software applications and systems.

Software Configuration Management – Applicable to all aspects of software development from design to delivery specifically focused on the control of all work products and artifacts generated during the development process. Several solutions on the market provide the integration of the software configuration management functions.

Version Management – Refers to tracking and controlling versions of files. Version Management includes capabilities such as labeling, branching, merging, version content comparisons, and security and permission management across version-controlled projects.

Defect Tracking – Refers to the identification, assignment, and management of discovered defects within an application, product or solution. Defect tracking tools provide searchable defect data to identify urgent and related defects or bugs. The architecture should be built to facilitate the pushing of software patches across the enterprise.

Issue Management – Refers to the management of business, technical, and infrastructure issues throughout the entire lifecycle of a project.

Task Management – Requirements, testing, and issues assignments are transformed into prioritized tasks. Task Management tools provide automation features for managing, delivering, assigning, reminding, and collaborating task management and execution.

Change Management – Refers to the management of application code and content changes across the software development lifecycles.

Deployment Management – Refers to the capability of software delivery to remote networked desktops, servers, and mobile devices across an enterprise. Deployment automation tools provide centralized and accelerated delivery of applications to users via push technologies, eliminating the need for manual installation and configuration.

Requirements Management and Traceability – Consists of information discovery, capture, storage and dissemination. Requirements management reduces software development costs and associated risks through documenting, measuring, and analyzing deviations to project requirements. Traceability refers to tracking requirements artifacts to their source, and changes in requirements to include the impact analysis of the change. Requirements traceability is an integral component in quality software implementation and the management of document succession.

Test Management – The consolidation of all testing activities and results. Test Management activities include test planning, designing (test cases), execution, reporting, code coverage, and heuristic and harness development.

Functional Testing – This type of test focuses on any requirements that can be traced directly to use cases (or business functions), business rules, and design.

Business Cycle Testing – Refers to the emulation of activities performed over a period of time that is relevant to the application under test.

Usability Testing (508 Testing) – Refers to a test to ensure that the application navigation, functionality, and GUI allow a user to effectively and efficiently do their work in a way that they are satisfied with the application.

Performance Profiling – Refers to a performance test that measures and evaluates response times and transaction rates.

Load/Stress/Volume Testing – Refers to tests that measure and evaluate how a system performs and functions under varying workloads, large amounts of data and/or resource utilization.

Security and Access Control Testing – Focuses on the technical, administrative and physical security controls that have been designed into the system architecture in order to provide confidentiality, integrity and availability.

Reliability Testing – Refers to the verification that failover methods are invoked properly and the system recovers properly.

Configuration Testing – Refers to a test to ensure that the application or system can handle all hardware and software variables and requirements that have been defined.

Installation Testing – Refers to the verification that the software installation process works properly in different environments and among varying conditions.

Modeling – The process of representing entities, data, business logic, and capabilities for aiding in software engineering.

Unified Modeling Language (UML) – A general-purpose notational language for specifying and visualizing complex software, especially large, object-oriented projects.

IDEF0 - IDEF0 Function Modeling, is the standard that describes the IDEF0 modeling language semantics and syntax, as well as associated rules and techniques, for developing structured graphical representations of a system or enterprise. The DoD Architecture Framework is evolving to encourage the use of object-oriented modeling methods over the use of methods based on structured analysis.

IDEF1X - Integrated Definition for Information Modeling (IDEF1X) is used to produce a graphical information model that represents the structure and semantics of information within an environment or system. FIPS PUB 184 is the standard that describes the IDEF1X modeling language (semantics and syntax) and associated rules and techniques. Use of this standard permits the construction of semantic data models, which support the management of data as a resource, the integration of information systems, and the building of relational databases.

IDEF1X97 - IDEF1X97 is being developed by the IEEE IDEF1X Standards Working group of the IEEE 1320.2 Standards Committee. The standard describes two styles of the IDEF1X model. The key-style is used to produce information models that represent the structure and semantics of data within an enterprise and is backward-compatible with the U.S. Government's Federal Standard for IDEF1X, FIPS PUB 184. The identity-style is a wholly new language that provides system designers
and developers with a robust set of modeling capabilities covering all static and many dynamic aspects of the emerging object model. This identity-style can, with suitable automation support, be used to develop a model that is an executable prototype of the target object-oriented system. The identity-style can be used in conjunction with emerging dynamic modeling techniques to produce full object-oriented models.

Data Architecture - Implementation of the DoD Data Architecture (DDA) will be interpreted to mean that it will serve as the logical reference model database schema defining the names, representations, and generalized relations of data within DoD systems.

Case Management - Computer Aided Software Engineering (CASE) software that provides a development environment for programming teams. CASE systems offer tools to automate, manage, and simplify the development process.

Database / Storage

Database / Storage refers to a collection of programs that enables storage, modification, and extraction of information from a database, and various techniques and devices for storing large amounts of data.

Database – Refers to a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database management system (DBMS) is a software application providing management, administration, performance, and analysis tools for databases.

Storage – Storage devices are designed to provide shared storage access across a network. These devices provide extended storage capabilities to the network with reduced costs compared to traditional file servers.

Network-Attached Storage (*NAS*) – A NAS device is a server that is dedicated to nothing more than file sharing.

Storage Area Network (SAN) – A SAN is a high-speed sub-network of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data.

Hardware / Infrastructure

Defines the physical devices, facilities and standards that provide the computing and networking within and between enterprises.

Servers / Computers – This refers to the various types of programmable machines which are capable of responding to sets of instructions and executing programs.

Enterprise Server – A computer or device on a network that manages network resources and shared applications for multiple users.

Mainframe – A very large computer capable of supporting hundreds, or even thousands, of users simultaneously. Mainframes support simultaneous programs.

Embedded Technology Devices – This refers to the various devices and parts that make up a server or computer as well as devices that perform specific functionality outside of a server or computer.

Random Access Memory (RAM) – A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers.

Hard Disk Drive – Refers to the area of a computer that where data is stored.

Microprocessor - A silicon chip that contains a CPU. In the world of personal computers, the terms microprocessor and CPU are used interchangeably. At the heart of all personal computers and most workstations sits a microprocessor.

Redundant Array of Independent Disks (RAID) – An assembly of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers. RAID is generally configured as mirrored or striped. Mirrored RAID (Level 1) provides a fail-over drive. Striped RAID (Levels 0, 3, and 5) write data across multiple disk drives so that a single disk failure can be recovered from the data on the remaining drives. There are three (3) types of RAID systems: failure-resistant disk systems (that protect against data loss due to disk failure), failure-tolerant disk systems (that protect against loss of data access due to failure of any single component), and disaster-tolerant disk systems (that consist of two or more independent zones, either of which provides access to stored data).

Peripherals – Computer devices that are not part of the essential computer (i.e. the memory and microprocessor). Peripheral devices can be external and internal.

Printer - Devices that print text or illustrations on paper. There are many different types of printers.

Scanner - Devices that can read text or illustrations printed on paper and translate the information into a form the computer can use. A scanner works by digitizing an image -- dividing it into a grid of boxes and representing each box with either a zero or a one, depending on whether the box is filled in.

Wide Area Network (WAN) - A data network typically extending a LAN outside a building or beyond a campus. Typically created by using bridges or routers to connect geographically separated LANs. WANs include commercial or educational dial-up networks such as CompuServe, InterNet and BITNET.

Frame Relay - packet-switching protocol for connecting devices on a Wide Area Network (WAN). Frame Relay networks in the U.S. support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds.
Asynchronous Transfer Mode (ATM) - A high bandwidth, high speed, controlled-delay, fixed-size packet switching and transmission system integrating multiple data types (voice, video, and data). Uses fixed-size packets also known as "cells" (ATM is often referred to as "cell relay").

Synchronous Optical Network Transmission (SONET) - Synchronous Optical Network (SONET) is a telecommunications transmission standard for use over fiber optic cable. SONET is the North American subset of the ITU standardized interfaces, and includes a hierarchical addressing scheme, multiple–structure optical parameters, and service mapping.

Local Area Network (LAN) - A network that interconnects devices over a geographically small area, typically in one building or a part of a building. The most popular LAN type is Ethernet. LANs allow the sharing of resources and the exchange of video and data.

Ethernet - local–area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps, 100 Mbps (Fast Ethernet) or 1 Gbps (gigabit Ethernet). The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.

Token Ring - A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.

Virtual LAN (VLAN) - A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Network Devices / Standards - A group of stations (computers, telephones, or other devices) connected by communications facilities for exchanging information. Connection can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (i.e. fiber optic cable) or wireless (i.e. satellite).

Hub - A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Switch - In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

Router - A device or setup that finds the best route between any two networks, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

Network Interface Card (NIC) - Often abbreviated as NIC, an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

Transceivers - Short for *transmitter-receiver,* a device that both transmits and receives analog or digital signals. The term is used most frequently to describe the component in local–area networks (LANs) that actually applies signals onto the network wire and detects signals passing through the wire. For many LANs, the transceiver is built into the network interface card (NIC). Some types of networks, however, require an external transceiver.

Gateway - Gateways are points of entrance to and exit from a communications network. Viewed as a physical entity, a gateway is that node that translates between two otherwise incompatible networks or network segments.

Integrated Services Digital Network (ISDN) – ISDN is a system of digital phone connections that has been available for more than a decade. This system allows data to be transmitted simultaneously across the world using end-to-end digital connectivity.

T1/T3 - T1 service delivers 1.544 Mbps. Typically channelized into 24 DS0s, each capable of carrying a single voice conversation or data stream. The European T1 or E1 transmission rate is 2.048 Mbps. A T3 circuit communicates at 45 Mbps, or 28 T1 lines.

Digital Subscriber Line (DSL) - Refers collectively to all types of digital subscriber lines, the two main categories being ADSL and SDSL. Two other types of xDSL technologies are High-data-rate DSL (HDSL) and Very high DSL (VDSL).

Firewall – This refers to the network device that is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. There are several types of firewall techniques and firewalls may implement one or more simultaneously. Packet filtering inspects inbound and outbound packets, validating against defined business rules. Application gateways apply security rules against applications. Circuit-level gateways apply security rules against physical connection attempts to and from the network. Proxy servers mask the internal requestor by inspecting and augmenting the packet header. Four common architectures of firewalls include the packet filtering router, the screened host firewall system, the dual homed host firewall, and the screened subnet firewall (with a DMZ), which is one of the most secure implementations.

Video Conferencing - Communication across long distances with video and audio contact that may also include graphics and data exchange. Digital video transmission systems typically consist of camera, codec (coder-decoder), network access equipment, network, and audio system.

Bridge - a bridge connects three or more conference sites so that they can simultaneously pass data, voice, or video. Videoconferencing bridges are often called MCUs (multipoint conferencing units).

CODEC - a video codec converts analog video signals from a video camera to digital signals for transmission over digital circuits, and then converts the digital signals back to analog signals for display.

Receiver - An electronic device which enables a particular videoconference signal to be separated from all others being received by an earth station, and converts the signal format into a format for video, voice or data.

Satellite Communications - The basic elements of satellite communications are a space segment, a control segment, and a terminal segment (air, ship, ground, etc.). An implementation of a typical satellite link will require the use of satellite terminals, a user communications extension, and military or commercial satellite resources.

Global Positioning System (GPS) - The CJCS (CJCSI 6130.01A, 1998 CJCS Master Positioning, Navigation, and Timing Plan) has declared that the GPS will be the primary radionavigation system source of positioning, navigation and timing (PNT) for DoD. GPS is a space-based, worldwide, precise positioning, velocity, and timing system. It provides an unlimited number of suitably equipped passive users with a force-enhancing, common-grid, all-weather, continuous, three-dimensional PNT capability.

Military Satellite Communications - Military Satellite Communications (MILSATCOM) systems include those systems owned or leased and operated by DoD and those commercial satellite communications (SATCOM) services used by DoD.

Satellite State-of-Health Communication - National Space Policy directed DoD to lead U.S. government efforts to improve satellite operations interoperability among U.S. government agencies. The National Security Space Architect's Satellite Operations Architecture Team recommended a common set of standards for LDR satellite telemetry and commanding. These standards will allow DoD to share health and status resources with other U.S. Government agencies and with allies to enhance satellite operations while limiting costs. The standards provide a baseline for LDR communication of health and status information between a spacecraft and the ground. These standards are mandated for S-band communication, but may be applied more generally.

Radio Communications – The transmission and reception of radio signals.

Voice Communications – The transmission and reception of human voice signals.

Network Operations

Network Operations involves the capability for monitoring and managing systems and related infrastructure at an enterprise-level, the capability for managing user and asset identity and authentication at an enterprise-level, the capability for managing the configuration of systems and software at an enterprise-level, and the capability to assure that new and transitioned systems maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability.

System Management - Systems Management provides the capability to manage designated systems and information services. This includes: the capability to review and publish addresses of system objects; monitor the status of objects;

start, restart, reconfigure, or terminate network or system services; and detect loss of system objects in order to support automated fault recovery.

Service Level Management – Service Level Management provides the ability of a network to ensure that the predetermined traffic and service requirements of network and service elements (e.g., end-system, router, or an application) can be satisfied.

Network Management - Network Management provides the capability to manage designated networks. This includes: controlling the network's topology; dynamically segmenting the network into multiple logical domains; maintaining network routing tables; monitoring the network load; and making routing adjustments to optimize throughput.

COMPONENT FRAMEWORK

The Component Framework Area, as illustrated in **Figure 7**, defines the underlying foundation and technical elements by which Service Components are built, integrated and deployed across Component-Based and Distributed Architectures. The Component Framework consists of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. This includes, but is not limited to, modules that are designed to interoperate with each other at runtime. Components can be large or small, written by different programmers using different development environments and may be platform independent. Components can be executed on stand-alone machines, a LAN, Intranet or on the Internet.

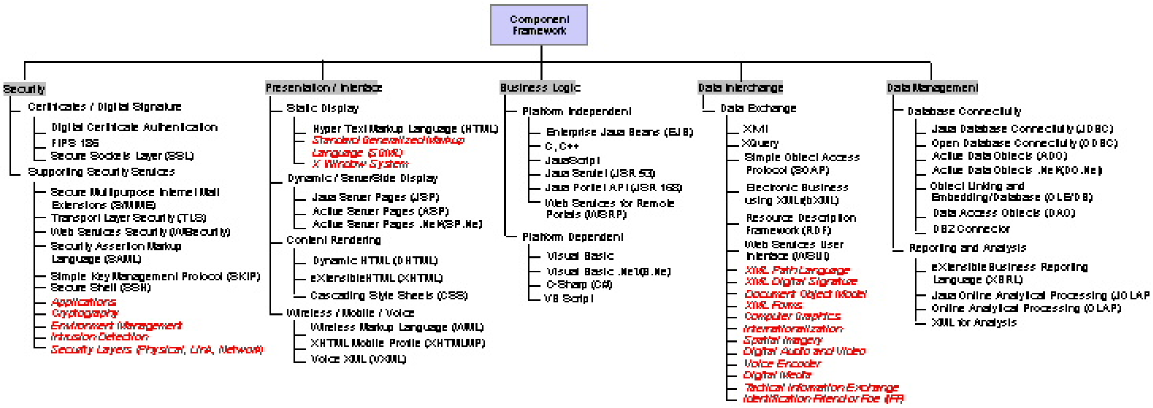

Component Framework
Security
Certificates / Digital Signature
Digital Certificate Authentication
FIPS 186
Secure Sockets Layer (SSL)
Supporting Security Services
Secure Multipurpose Internet Mail Extensions (S/MIME)
Transport Layer Security (TLS)
Web Services Security (WS-Security)
Security Assertion Markup Language (SAML)
Simple Key Management Protocol (SKIP)
Secure Shell (SSH)
Applications
Cryptography
Environment Management
Intrusion Detection
Security Layers (Physical, Link, Network)
Presentation / Interface
Static Display
Hyper Text Markup Language (HTML)
Standard Generalized Markup Language (SGML)
X Window System
Dynamic / Server-Side Display
Java Server Pages (JSP)
Active Server Pages (ASP)
Active Server Pages .Net (ASP.Net)
Content Rendering
Dynamic HTML (DHTML)
eXtensible HTML (XHTML)
Cascading Style Sheets (CSS)
Wireless / Mobile / Voice
Wireless Markup Language (WML)
XHTML Mobile Profile (XHTMLMP)
Voice XML (VXML)
Business Logic
Platform Independent
Enterprise Java Beans (EJB)
C, C++
JavaScript
Java Servlet (JSR 53)
Java Portlet API (JSR 168)
Web Services for Remote Portals (WSRP)
Platform Dependent
Visual Basic
Visual Basic .Net (VB.Net)
C-Sharp (C#)
VB Script
Data Interchange
Data Exchange
XMI
XQuery
Simple Object Access Protocol (SOAP)
Electronic Business using XML (ebXML)
Resource Description Framework (RDF)
Web Services User Interface (WSUI)
XML Path Language
XML Digital Signature
Document Object Model
XML Forms
Computer Graphics
Internationalization
Spatial Imagery
Digital Audio and Video
Voice Encoder
Digital Media
Tactical Information Exchange
Identification Friend or Foe (IFF)
Data Management
Database Connectivity
Java Database Connectivity (JDBC)
Open Database Connectivity (ODBC)
Active Data Objects (ADO)
Active Data Objects .Net (ADO.Net)
Object Linking and Embedding/Database (OLE/DB)
Data Access Objects (DAO)
DB2 Connector
Reporting and Analysis
eXtensible Business Reporting Language (XBRL)
Java Online Analytical Processing (JOLAP
Online Analytical Processing (OLAP)
XML for Analysis

Figure 7: Component Framework Service Area

The Component Framework Service Categories, Standards, and Specifications are defined below:

Security

Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability. Biometrics, two-factor identification, encryption, and technologies based on the NIST FIPS-140 standards are evolving areas of focus. http://csrc.nist.gov/cryptval/

Certificates / Digital Signature - Software used by a certification authority (CA) to issue digital certificates and secure access to information. The evolution of Public Key Infrastructure (PKI) is based on the verification and authentication of the parties involved in information exchange.

> *Digital Certificate Authentication* – Authentication implementation for controlling access to network and internet resources through managing user identification. An electronic document – a digital certificate – is issued and used to prove identity and public key ownership over the network or internet.
>
> *Secure Sockets Layer (SSL)* - An open, non-proprietary protocol for securing data communications across computer networks. SSL is sandwiched between the application protocol (such as HTTP, Telnet, FTP, and NNTP) and the connection protocol (such as TCP/IP, UDP). SSL provides server authentication, message integrity, data encryption, and optional client authentication for TCP/IP connections.

Supporting Security Services - These consist of the different protocols and components to be used in addition to certificates and digital signatures.

> *Secure Multipurpose Internet Mail Extensions (S/MIME)* - Provides a consistent way to send and receive secure MIME data. Based on the Internet MIME standard, S/MIME provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and data confidentiality (using encryption). S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP.
>
> *Transport Layer Security (TLS)* - Standard for the next generation SSL. TLS provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
>
> *Web Services Security (WS-Security)* - Describes enhancements to SOAP messaging to provide message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies including X.509, Kerberos, and SAML.
>
> *Security Assertion Markup Language (SAML)* - An XML-based framework for exchanging security information expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. SAML is expected to play a key role in the Federal-wide e-authentication initiative, and is supported by the Liberty Alliance and WS-Security.
>
> *Simple Key Management Protocol (SKIP)* – A protocol developed by Sun Microsystems to handle key management across IP networks and VPNs.

Secure Shell (SSH) – A strong method of performing client authentication. Because it supports authentication, compression, confidentiality and integrity, SSH is used frequently on the Internet. SSH has two important components, RSA certificate exchange for authentication and Triple DES for session encryption.

Applications - Mandated and emerging application standards (including Web browsing, e-mail, and operating system[OS]).

Cryptography - The asymmetric cryptography used to support the Public Key Infrastructure, which is a system of Certificate Authorities that perform some set of certificate management, archive management, key management, and token management functions for a community of users.

Environment Management - Environment management services integrate and manage the execution of platform services for particular applications and users. These services are invoked via an easy-to-use, high-level interface that enables users and applications to invoke platform services without having to know the details of the technical environment. The environment management service determines which platform service is used to satisfy the request and manages access to it through the API.

Intrusion Detection - An intrusion is an attempt to break into or misuse a computer system or network. An intrusion detection system, attempts to detect an intruder breaking into your system or a legitimate user misusing system resources. The intrusion detection system should run constantly on your system, working away in the background, and only notifying you when it detects something it considers suspicious or illegal. What is suspicious or illegal depends on the security policy you have established for the system.

Security Layers (Physical, Link, Network) - The physical layer, Layer 1 of the OSI 7 Layer Reference Model, provides the mechanical, electrical, functional, and procedural means to activate, maintain, and deactivate physical connections for bit transmission between data-link entities. The (data) link layer is layer 2 of the Open Systems Interconnect (OSI) 7 Layer Reference Model where a point-to-point communication channel connecting two sub–network relays is established. The Network layer is layer 3 of the Open Systems Interconnect (OSI) 7 Layer Reference Model.

Presentation / Interface

This defines the connection between the user and the software, consisting of the presentation that is physically represented on the screen.

Static Display - Static Display consists of the software protocols that are used to create a pre-defined, unchanging graphical interface between the user and the software.

Hyper Text Markup Language (HTML) - The language used to create Web documents and a subset of Standard Generalized Markup Language (SGML).

Standard Generalized Markup Language (SGML) - A standard methodology with formal syntax for adding information to a document relating to its structure and/or content by applying identifiers for elements of information in a neutral way, stored in a neutral form, independent of systems, devices, and applications. HTML and XML are examples of SGML-based document markup languages.

X Window System - For Portable Operating System Interface for Computer Environments (POSIX)-based systems, the Common Desktop Environment (CDE)/Motif provides a common set of desktop applications and management capabilities. CDE/Motif uses the underlying X-Windows system.

Dynamic / Server-Side Display - This consists of the software that is used to create graphical user interfaces with the ability to change while the program is running.

Content Rendering - This defines the software and protocols used for transforming data for presentation in a graphical user interface.

Wireless / Mobile / Voice - Consists of the software and protocols used for wireless and voice-enabled presentation devices.

Business Logic

Defines the software, protocol or method in which business rules are enforced within applications.

Platform Independent - Consists of all software languages that are able to execute and run on any type of operating system or platform.

Platform Dependent - Consists of the programming languages and methods for developing software on a specific operating system or platform.

Data Interchange

Define the methods in which data is transferred and represented in and between software applications.

Data Exchange – Data Exchange is concerned with the sending of data over a communications network and the definition of data communicated from one application to another. Data Exchange provides the communications common denominator between disparate systems.

XMI - Enables easy interchange of metadata between modeling tools (based on the OMG UML) and metadata repositories (OMG MOF based) in distributed heterogeneous environments. XMI integrates three key industry standards: XML, UML, and MOF. The integration of these three standards into XMI marries the best of OMG and W3C metadata and modeling technologies, allowing developers of distributed systems to share object models and other metadata over the Internet.

XQuery – A language used for processing and evaluating XML data. The XQuery language provides results of expressions allowing the use of evaluations to the implementation of XQuery.

XML Path Language - XPath is a language for addressing parts of an XML document, designed to be used by XSLT.

XML Digital Signature – A language for applying an XML-encoded digital signature within an XML document, rather than as separate data.

Document Object Model – A programmatic means for read/write random access to XML documents, There are different approaches for accessing XML data, e.g., the Simple API for XML (SAX) approach is used for sequential access and the Java Document Object Model (JDOM) approach is used for a Java-specific binding of Document Object Model (DOM).

XML Forms - XForms architecture separates purpose (semantics) from presentation (syntax), and associates the capabilities of XML and the ease of HTML for a wide range of devices.

Simple Object Access Protocol (SOAP) – SOAP provides HTTP/XML–based remote procedure call capabilities for XML Web Services.

Electronic Business using XML (ebXML) - A modular suite of specifications that enables enterprises to conduct business over the internet: exchanging business messages, conducting trading relationships, communicating data in common terms and defining and registering business processes.

Resource Description Framework (RDF) - RDF provides a lightweight ontology system to support the exchange of knowledge on the Web. It integrates a variety of web-based metadata activities including sitemaps, content ratings, stream channel definitions, search engine data collection (web crawling), digital library collections, and distributed authoring, using XML as interchange syntax. RDF is the foundation for the Semantic Web envisioned by Tim Berners-Lee - an extension of the current web in which information is given well-defined meaning, better enabling computers and people to work in cooperation.

Web Services User Interface (WSUI) - WSUI uses a simple scheme for describing a WSUI "component" that can be used in a portal to call backend SOAP and XML services. WSUI uses XSLT stylesheets to construct user-facing views to enable users to interact with the services.

Computer Graphics - These services are supported by device-independent descriptions of the picture elements for vector and raster graphics. The International Organization for Standardization (ISO) Joint Photographic Expert Group (JPEG) standard describes several alternative algorithms for the representation and compression of raster images, particularly for imagery; JPEG images may be transferred using the JPEG File Interchange Format (JFIF). Graphics Interchange Format (GIF) and JFIF are de facto standards for exchanging graphics and images over an Internet. GIF supports lossless-compressed images with up to 256 colors and short animation segments. Note that Unisys owns a related patent, which requires a license for software that writes the GIF format.

Internationalization - A set of services and interfaces that allow a user to define, select, and change between different culturally related application environments supported by the particular implementation. These services include character sets, data representation, cultural convention, and native-language support.

Spatial Imagery - Geospatial services are also referred to as mapping, charting, and geodesy (MC&G) services.

Digital Audio and Video - Video support services specifies the structure and data formats for the production, exchange, transmission, or use of digital video data. Effective compression of audio data depends not only upon data compression techniques but also upon the application of a psycho-acoustic model that predicts which sounds humans are likely to be able to hear or not hear in given situations.

Voice Encoder - Common high performance voice encoding algorithms for use across the communications infrastructure.

Digital Media - Data Interchange Storage Media.

Tactical Information Exchange - Bit-oriented fixed and variable formatted Tactical Data Link (TDL) standards which allow real- or near-real-time tactical, digital-information exchange among air, ground, and maritime components of United States (U.S.), North Atlantic Treaty Organization (NATO), other allies, and friendly nations. Character–based information standards, which provide common, human-readable, and media-independent messages used for planning and execution in joint and combined operations among U.S. forces, NATO, other allies, and friendly nations.

Identification Friend or Foe (IFF) - The primary function of Identification Friend or Foe (IFF) is to establish the identity of all friendly systems within the surveillance volume of surface-to-air, air-to-air, and some air-to-ground Weapon System platforms. The need for friend identification is to permit tactical action against all foe (non-friendly) systems and to avoid tactical action against friendly systems. This need is a key element in modern combat, as an object detected by a sensor, even beyond visual range, has to be identified and classified as early as possible so that, if necessary, either an appropriate defense can be prepared against the foe or that steps can be taken to prevent the friend from being engaged/ attacked by friendly forces.

Data Management

The management of all data/information in an organization includes data administration, the standards for defining data and the way in which people perceive and use it.

Database Connectivity - Defines the protocol or method in which an application connects to a data–store or database.

Reporting and Analysis - Consists of the tools, languages and protocols used to extract data from a data–store and process it into useful information.

SERVICE INTERFACE AND INTEGRATION

The Service Interface and Integration Area, as illustrated in **Figure 8**, defines the discovery, interaction and communication technologies joining disparate systems and information providers. Component-based architectures leverage and incorporate Service Interface and Integration specifications to provide interoperability and scalability.

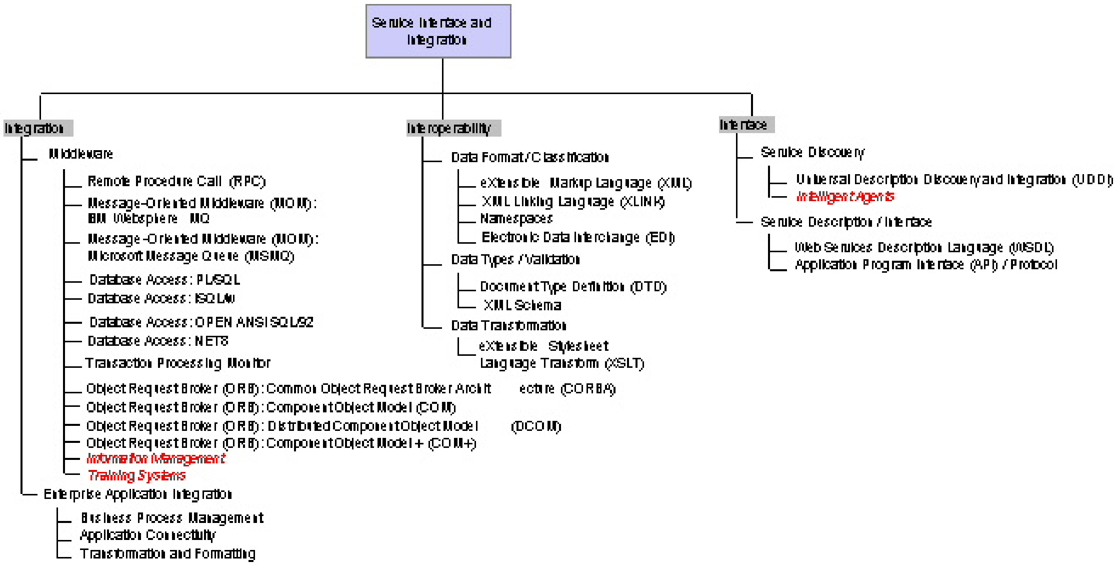

Service Interface and Integration
Integration
Middleware
Remote Procedure Call (RPC)
Message-Oriented Middleware (MOM): IBM Websphere MQ
Message-Oriented Middleware (MOM): Microsoft Message Queue (MSMQ)
Database Access: PL/SQL
Database Access: ISQL/w
Database Access: OPEN ANSI SQL/92
Database Access: NET8
Transaction Processing Monitor
Object Request Broker (ORB): Common Object Request Broker Architecture (CORBA)
Object Request Broker (ORB): Component Object Model (COM)
Object Request Broker (ORB): Distributed Component Object Model (DCOM)
Object Request Broker (ORB): Component Object Model + (COM+)
Information Management
Training Systems
Enterprise Application Integration
Business Process Management
Application Connectivity
Transformation and Formatting
Interoperability
Data Format / Classification
eXtensible Markup Language (XML)
XML Linking Language (XLINK)
Namespaces
Electronic Data Interchange (EDI)
Data Types / Validation
Document Type Definition (DTD)
XML Schema
Data Transformation
eXtensible Stylesheet Language Transform (XSLT)
Interface
Service Discovery
Universal Description Discovery and Integration (UDDI)
Intelligent Agents
Service Description / Interface
Web Services Description Language (WSDL)
Application Program Interface (API) / Protocol

Figure 8: Service Interface and Integration Area

The Service Interface and Integration Categories, Standards, and Specifications are defined below:

Integration

Integration defines the software services enabling elements of distributed business applications to interoperate. These elements can share function, content, and communications across heterogeneous computing environments. In particular, service integration offers a set of architecture services such as platform and service location transparency, transaction management, basic messaging between two points, and guaranteed message delivery.

Middleware – Middleware increases the flexibility, interoperability, and portability of existing infrastructure by linking or “gluing” two otherwise separate applications.

Database Access: OPEN ANSI SQL/92 – SQL is the information processing industry standard language of relational database management systems (RDMS). ANSI X3.135-1992 (also referred to as SQL-92 and ANSI SQL) is the industry standard for Database Language SQL. This standard promotes the portability and interoperability of database application programs and facilitates maintenance of database systems across heterogeneous data processing environments. SQL-92 provides a standardized way for embedding SQL statements into application development languages. Database Access provides access to and across multiple database technologies in a distributed environment. Database Access is provided through the use of native database Application Programming Interfaces (APIs), client–side APIs, or server–side database gateways.

Transaction Processing Monitor – Software providing synchronous messaging and queuing along with other transaction management services designed to support the efficient processing of high volumes of transactions. Core services include load balancing, rollback/commit, and recovery. Transaction Processing provides cost-effective scalability to applications and database systems by managing and throttling transactions on behalf of the database system.

Object Request Broker (ORB): Common Object Request Broker Architecture (CORBA) – An architecture that enables objects to communicate with one another regardless of what programming language they were written in or what operating system they're running on. Object Request Broker (ORB) is a technology enabling distributed objects to communicate and exchange data with remote objects. ORB encapsulates the locality and implementation of the objects, allowing users to develop applications that leverage components by accessing the components interface.

Information Management - Central to most systems is the sharing of information between applications. The information management services provide for the independent management of information shared by multiple applications.

Training Systems – Training Systems provide for an integrated environment for education, training, and decision support. A growing number of technical standards for this field are in varying stages of
development.

Enterprise Application Integration – Refers to the processes and tools specializing in updating and consolidating applications and data within an enterprise. EAI focuses on leveraging existing legacy applications and data sources so that enterprises can add and migrate to current technologies.

Business Process Management – This process is responsible for the definition and management of cross-application business processes across the enterprise and/or between enterprises.

Application Connectivity – This process provides reusable, non-invasive connectivity with packaged software. This connectivity is provided by uni- or bi-directional adapters.

Transformation and Formatting – This process is responsible for the conversion of data, message content, information structure, and syntax to reconcile differences in data amongst multiple systems and data sources.

Interoperability

Interoperability defines the capabilities of discovering and sharing data and services across disparate systems and vendors.

Data Format / Classification – Defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word processing, graphics, executable program, etc.). Each format defines its own layout of the data. The file format for text is the simplest.

eXtensible Markup Language (XML) – XML has emerged as the standard format for web data, and is beginning to be used as a common data format at all levels of the architecture. Many specialized vocabularies of XML are being developed to support specific Government and Industry functions.

XML Linking Language (XLINK) – A language used to modify XML documents to include links, similar to hyperlinks, between resources. XLINK provides richer XML content through advanced linking integration with information resources.

Namespaces – Namespaces are qualified references to URI (Uniform Resource Identifier) resources within XML documents.

Electronic Data Interchange (EDI) - Defines the structure for transferring data between enterprises. EDI is used mainly used for purchase-related information. ANSI X.12 refers to the approved EDI standards.

Data Types / Validation – Refers to specifications used in identifying and affirming common structures and processing rules. This technique is referenced and abstracted from the content document or source data.

Document Type Definition (DTD) – DTD is used to restrict and maintain the conformance of an XML, HTML, or SGML document. The DTD provides definitions for all tags and attributes within the document and the rules for their usage. Alterations to the document are validated with the referenced DTD.

XML Schema – XML Schemas define the structure, content, rules and vocabulary of an XML document. XML Schemas are useful in automation through embedding processing rules.

Data Transformation - Data Transformation consists of the protocols and languages that change the presentation of data within a graphical user interface or application.

eXtensible Stylesheet Language Transform (XSLT) - Transforms XML document from one schema into another. Used for data transformation between systems using different XML schema, or mapping XML to different output devices.

Interface
Interface defines the capabilities of communicating, transporting and exchanging information through a common dialog or method. Delivery Channels provide the information to reach the intended destination, whereas Interfaces allow the interaction to occur based on a predetermined framework.

Service Discovery - Defines the method in which applications, systems or web services are registered and discovered.

Universal Description Discovery and Integration (UDDI) - UDDI provides a searchable registry of XML Web Services and their associated URLs and WSDL pages.

Intelligent Agent – An autonomous software component that uses intelligence to do an assigned task; for example, searching through incoming mail and highlighting items related to a certain subject.

Service Description / Interface - Defines the method for publishing the way in which web services or applications can be used.

Web Services Description Language (WSDL) - WSDL is an XML based Interface Description Language for describing XML Web Services and how to use them.

Application Program Interface (API) / Protocol - A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol. APIs are implemented by writing function calls in the program, which provide the linkage to the required subroutine for execution. Thus, an API implies that some program module is available in the computer to perform the operation or that it must be linked into the existing program to perform the tasks.

CHAPTER 3. MAPPING BETWEEN DISR AND FEA TRM

A set of high-level mappings has been established (see **Figures 9**, **10** and **11** below) to enable DoD Program Managers to readily see the relationships between the DoD EA TRM technology categories and those currently used in the DISR. These mappings are shown in one direction using green lines, from the DISR category to the DoD EA TRM category. The box on the end of each mapping line shows the target DoD EA TRM category, and multiple DISR categories may map to that target.

Program Managers can use this quick mapping to see relevant TRM categories. To examine the mappings of specific DISR specifications, the detailed tables found in the attached spreadsheet (Appendix A) would be used.

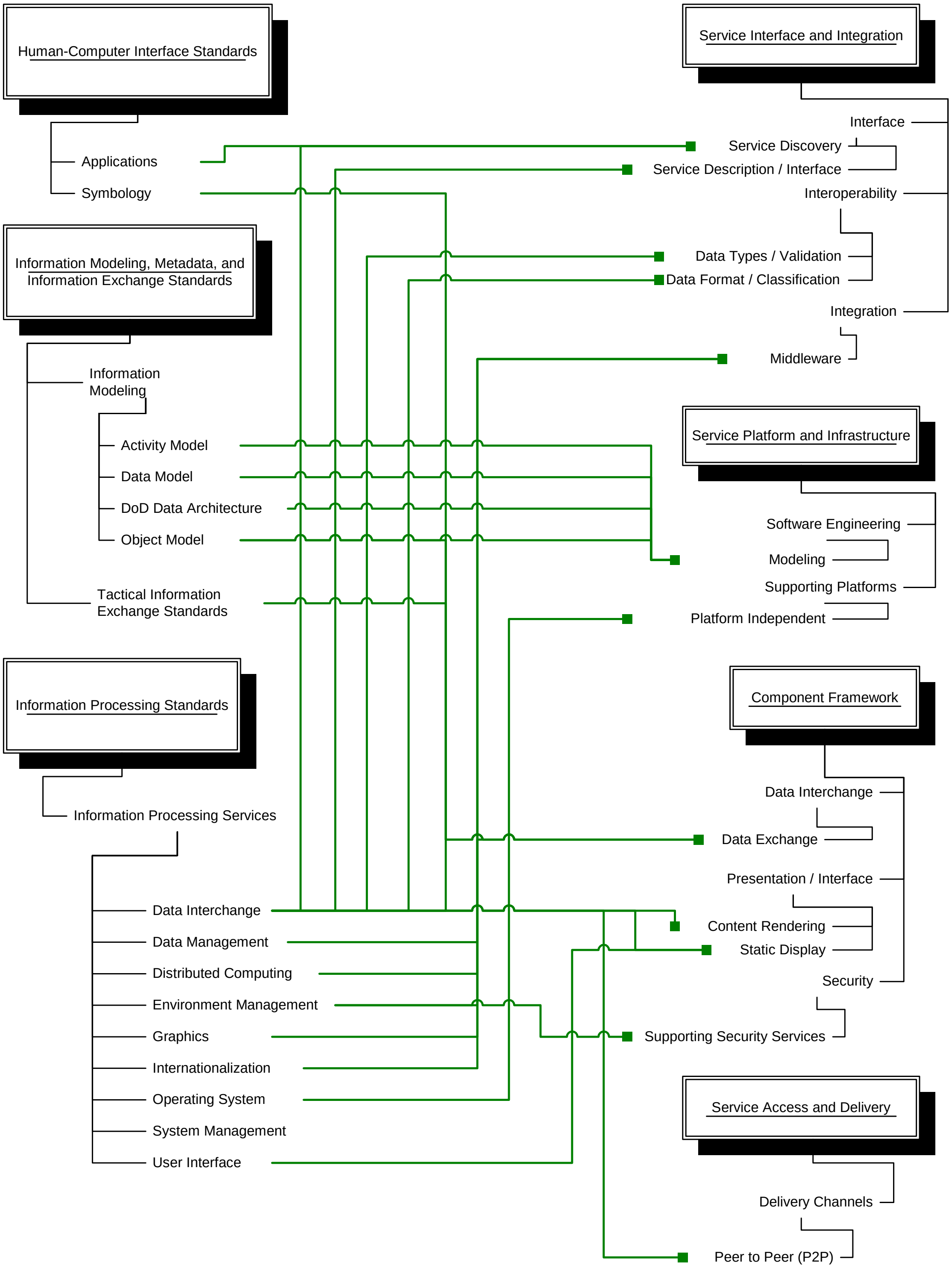


Figure 9: DISR High-Level Mappings to FEA TRM, Part 1

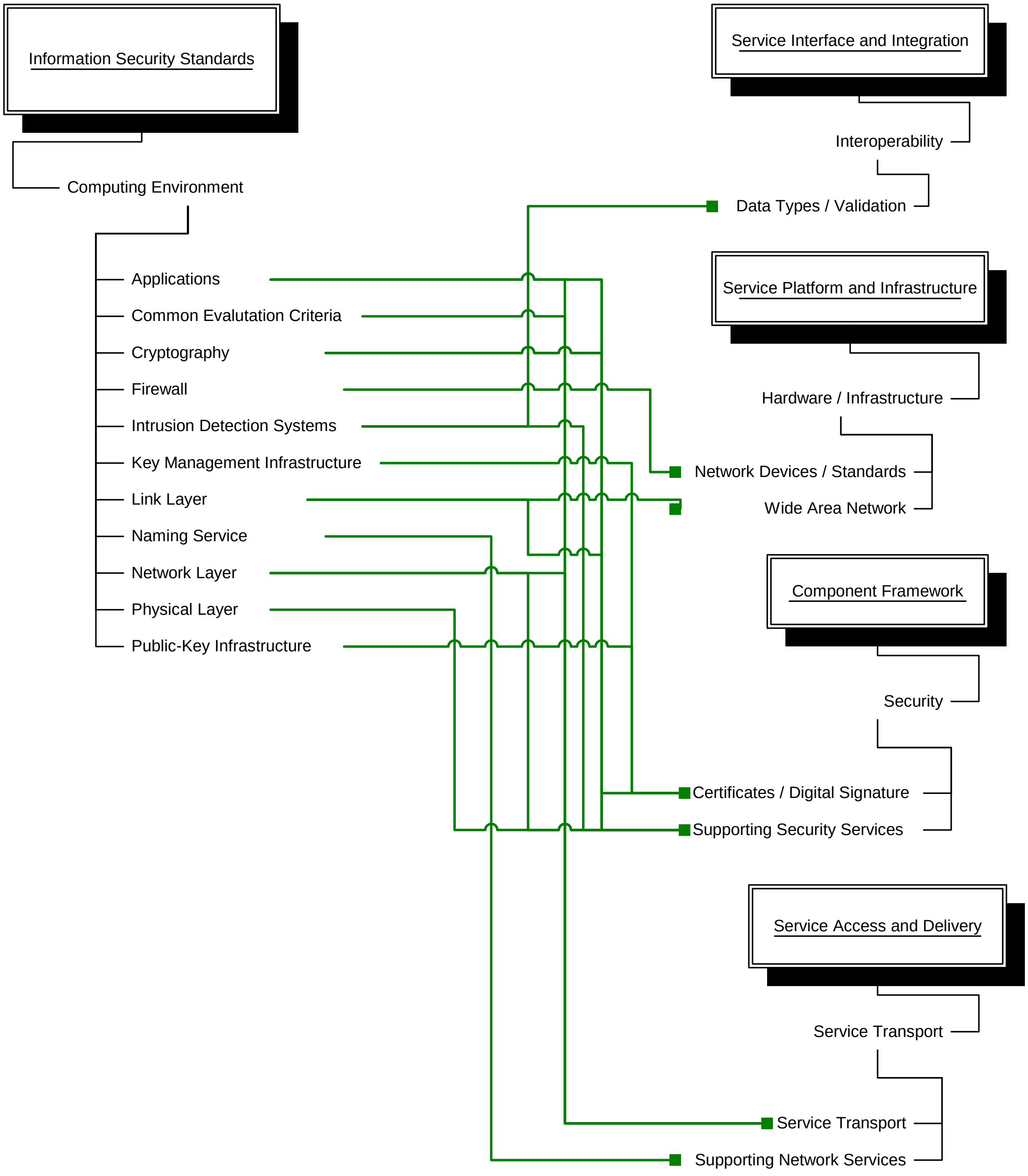

Information Security Standards
Computing Environment
Applications
Common Evalutation Criteria
Cryptography
Firewall
Intrusion Detection Systems
Key Management Infrastructure
Link Layer
Naming Service
Network Layer
Physical Layer
Public-Key Infrastructure
Service Interface and Integration
Interoperability
Data Types / Validation
Service Platform and Infrastructure
Hardware / Infrastructure
Network Devices / Standards
Wide Area Network
Component Framework
Security
Certificates / Digital Signature
Supporting Security Services
Service Access and Delivery
Service Transport
Service Transport
Supporting Network Services

Figure 10: DISR High-Level Mappings to FEA TRM, Part 2

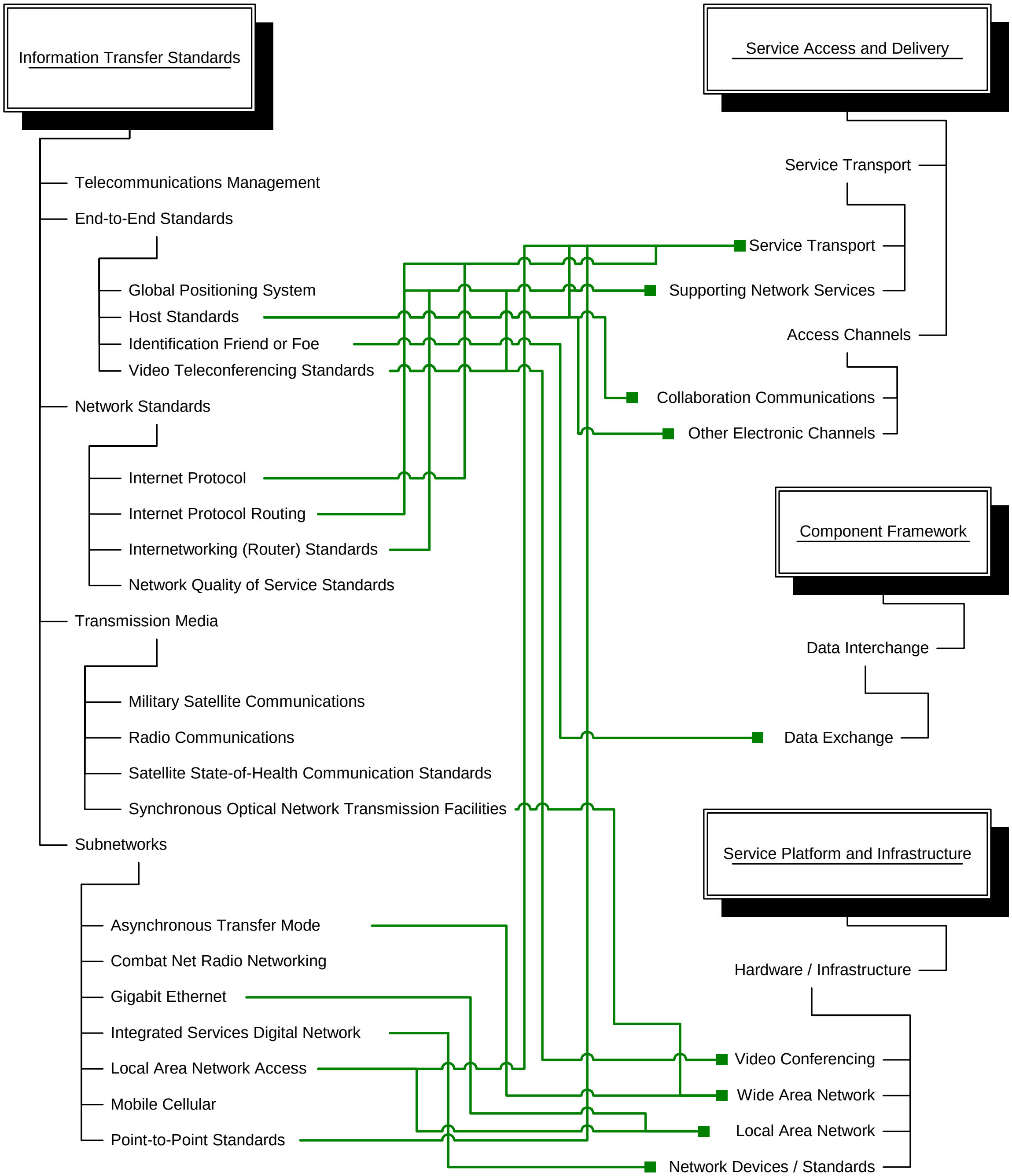

Information Transfer Standards
Telecommunications Management
End-to-End Standards
Global Positioning System
Host Standards
Identification Friend or Foe
Video Teleconferencing Standards
Network Standards
Internet Protocol
Internet Protocol Routing
Internetworking (Router) Standards
Network Quality of Service Standards
Transmission Media
Military Satellite Communications
Radio Communications
Satellite State-of-Health Communication Standards
Synchronous Optical Network Transmission Facilities
Subnetworks
Asynchronous Transfer Mode
Combat Net Radio Networking
Gigabit Ethernet
Integrated Services Digital Network
Local Area Network Access
Mobile Cellular
Point-to-Point Standards
Service Access and Delivery
Service Transport
Service Transport
Supporting Network Services
Access Channels
Collaboration Communications
Other Electronic Channels
Component Framework
Data Interchange
Data Exchange
Service Platform and Infrastructure
Hardware / Infrastructure
Video Conferencing
Wide Area Network
Local Area Network
Network Devices / Standards

Figure 11: DISR High-Level Mappings to FEA TRM, Part 3

CHAPTER 4. DOD EA TRM USE AND MAINTENANCE

BENEFITS OF THE DOD EA TRM

By mapping baseline architectures to the DoD EA TRM, strategies for migrating to net-centricity and service-oriented architectures will likely be more readily visible. Upon "publishing" this mapping in conjunction with a mapping to the DoD EA SRM, DoD Components are offered the ability to discover workable capability and technology configurations. Realizing and leveraging existing investments is a key benefit and driver of the DoD EA. Also, the DoD EA TRM is intended to align with the FEA TRM to assist Federal Agencies in optimizing re-use of IT capability and technology investments and to achieve the same optimization within DoD.

Aligning the layers of the DoD EA TRM and SRM to FEA technology, business (process or activity), and application reference models enables the categorization of an Agency's IT investments, assets and infrastructure by the common definition, organization, and purpose of the Service Specifications and Service Components in the FEA TRM and FEA SRM, respectively.

DOD IMPLEMENTATION OF THE TRM

The DoD EA TRM is composed of technology components that encompass an entire infrastructure – internal, external, and the connection in between. These components reside across the network and the application topology.

Many technology standards can exist within more than one partition of the physical networks that make up an enterprise infrastructure. An Agency TRM should specifically identify the technologies and products used within their enterprise as well as their physical or logical placement. To illustrate employment of the concepts above, the US Patent and Trademark Office (USPTO) is presented here as an example. They restructured their Agency TRM (USPTO TRM version 7) to better align their baseline and target architectures with the TRM. USPTO also conducts technology reviews in order to continue, contain, or retire technologies (a part of standards life cycle management) as necessary as they strive to achieve a components-based architecture.

USPTO claims three significant advantages with the implementation of their TRM in alignment with the FEA:

- Reduced infrastructure complexity through identification of standards and products
- Improved leveraging of innovative technology
- Increased access to information

The Federal government can benefit from the information gathered and efforts engaged by DoD (and other Agencies) through the "patterns" they establish of workable capabilities and technologies in meeting business and performance requirements. As Agencies begin assembling technology components, and determining the appropriate configurations to overcome specific performance gaps, certain technology patterns begin to emerge. These patterns, mapped to the SRM service components employed and performance goals (from the PRM) achieved, will also indicate specific environments where they succeed. Agencies can leverage the success of others in building their own architectures. **Figure 12** illustrates a sample pattern.

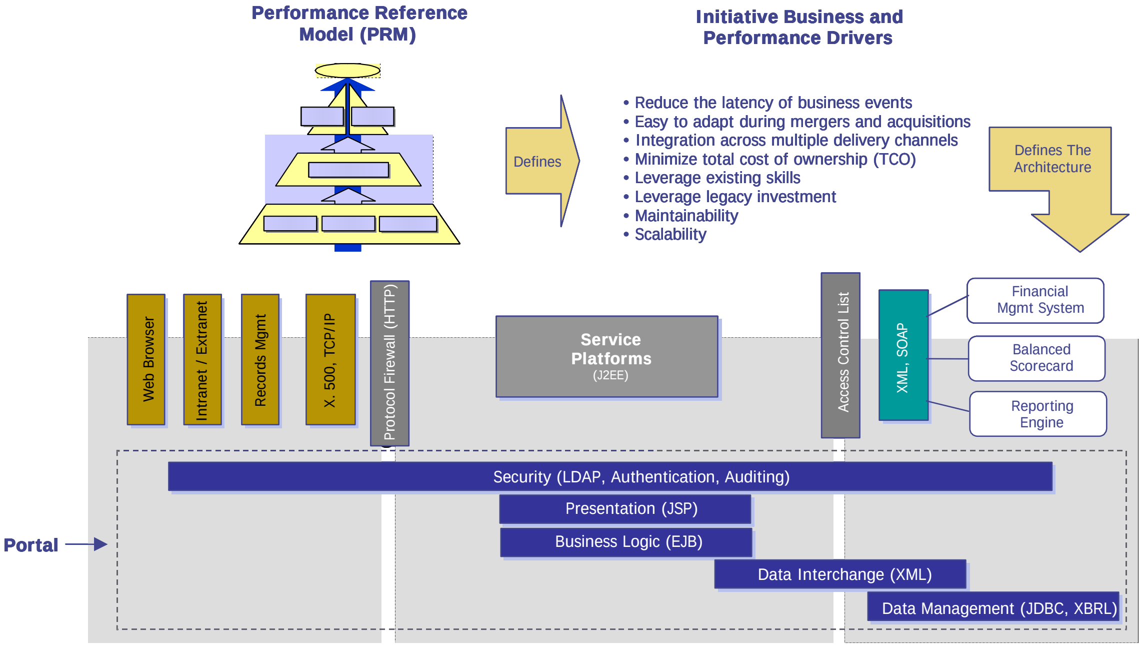

Performance Reference Model (PRM)
Initiative Business and Performance Drivers
Defines
• Reduce the latency of business events
• Easy to adapt during mergers and acquisitions
• Integration across multiple delivery channels
• Minimize total cost of ownership (TCO)
• Leverage existing skills
• Leverage legacy investment
• Maintainability
• Scalability
Defines The Architecture
Web Browser
Intranet / Extranet
Records Mgmt
X. 500, TCP/IP
Protocol Firewall (HTTP)
Service Platforms
(J2EE)
Access Control List
XML, SOAP
Financial Mgmt System
Balanced Scorecard
Reporting Engine
Security (LDAP, Authentication, Auditing)
Presentation (JSP)
Business Logic (EJB)
Data Interchange (XML)
Data Management (JDBC, XBRL)
Portal

Figure 12: Sample Pattern for Back Office Integration

Additionally, in the coming months and via separate documents, the FEA-PMO will look to provide some guidance on selection of various components and building secure infrastructures.

CHAPTER 4. DOD EA TRM ANALYSIS

DOD EA TRM AND FEA TRM COMPARISON

The most distinct difference between the DoD approach to a TRM and the FEA approach is the fact that the FEA identifies specific vendor products while DoD focuses on technical specIfications and tries to remain vendor-neutral. This is consistent with DoD's approach to fair competition in acquisition. For this reason, all product and standard recommendations have been clearly identified and moved to an appendix.

Most of the technologies essential to e-Government and citizen self-service in the Federal Enterprise Architecture are being utilized by the DoD in support of its net-centric operations and warfare. This is evidenced by the fact that no Core Service Areas or Service Categories needed to be added to the FEA TRM in order to capture the technologies applicable to the DoD. This also demonstrates the fundamental similarity between the Federal and DoD thrusts.

Other differences include the fact that DoD, by the nature of national security concerns and the special needs of a real-time battlefield, is itself a telecommunications service provider while the Federal government buys these services commercially. The technologies applied include all the elements of a typical commercial terrestrial network as well as satellites, radios and other mobile devices. In addition, technologies are needed to manage, secure and defend this complex and specialized network. DoD also utilizes a much wider range of multimedia and messaging technologies than does the Federal government, particularly in specialized spatial imagery and real-time tactical communications.

CONCLUSION

By mapping its architectures to the DoD EA TRM, the DoD community can gain significant value in its joint interoperability, portfolio and investment management initiatives. The identification of similar technology use across the Service Components can help establish cross service Communities of Interest, facilitate standard development, as well as joint interoperability. In addition, the use of a common, joint set of technology categories can help identify common areas of technology use, and therefore the potential to leverage enterprise-purchasing advantages.

RECOMMENDATIONS

The DoD EA TRM is in a preliminary state. It could significantly benefit from greater scrutiny across the technical community. It is not yet effectively organized to fully promote the adoption of net-centric technologies, or the development of net-centric enterprise services. Some elements in the TRM may not truly apply across the DoD as a whole, and may be best extracted into domain-specific extensions. Subsequent revisions of the DoD EA TRM should begin to address these deficiencies.

APPENDIX A. SPECIFICATION MAPPINGS

Appendix A is a spreadsheet that provides detailed, specification-by-specification mappings between the DoD specifications and the FEA TRM standards and specifications, and vice-versa. A standard describes a certain area of industry or government technology standardization. A specification is a version or specific implementation of a given standard. DoD focuses its technology analysis on specific specifications, while the FEA tends to focus on identifying standards.

Appendix A consists of two tables that were used to develop the DoD EA TRM:

- The first table consists of mappings from DISR and other DoD specifications to equivalent FEA TRM standards. Most of the specifications are derived directly from the DISR. When a specification comes from an alternative DoD source (such as the Business Enterprise Architecture technical view), that source is listed in parentheses at the end of the specification text. Where required to support DoD needs, logical extensions to the FEA standards have been proposed and marked in red. These extensions have been included in the DoD EA TRM.

- The second table consists of mappings from FEA TRM standards to equivalent DISR and other DoD specifications. This is the original table used in the DoD EA TRM analysis. As such, it can be used to examine gaps between the FEA and DoD approaches, sources of the references, and the applicable timeframe of the DoD technical specifications.